COMPLETE LISTING OF THE CLAIMS

Claim 1 (currently amended): A pseudo-random key generator for use within a cryptographic communication system, said pseudo-random key generator comprising:

a pseudo-random number generator for periodically generating a plurality of pseudo-random numbers, wherein a pseudo-random number is generated for every occurrence of a predetermined key change period;

a computer readable storage medium connected to said pseudo-random number generator;

a timing circuit operatively coupled to said pseudo-random number generator, said timing circuit includes a time/key initialization device and a timing source for providing current timing values,

wherein, upon initialization of the pseudo-random key generator, said timing source compares a current timing value with a predetermined crypto midnight initialization timing value, and transmits the difference to the time/key initialization device, which causes the pseudo-random number generator to ~~generate~~ cycle through a set of initialization pseudo-random numbers starting from the crypto midnight initialization timing value until a pseudo-random number is generated in sequence for all of the key change periods between the crypto midnight initialization timing value and the current timing value.

Claim 2 (previously presented): The pseudo-random key generator according to claim 1, wherein said timing circuit further includes a delta counter operatively coupled to said time/key initialization device.

Claim 3 (canceled)

Claim 4 (previously presented): The pseudo-random key generator according to claim 1, wherein said computer readable storage medium includes a PRN re-map table.

Claim 5 (previously presented): The pseudo-random key generator according to claim 1, wherein said computer readable storage medium includes a PRN re-map table.

Claim 6 (previously presented): The pseudo-random key generator according to claim 1, further comprising a read only computer readable storage medium connected to said timing circuit.

Claim 7 (previously presented): The pseudo-random key generator according to claim 6, wherein said read only computer readable storage medium includes:

the crypto midnight initialization timing value; and

the key change period value.

Claim 8 (previously presented): The pseudo-random key generator according to claim 6, wherein said computer readable storage medium includes an executable program, said executable program causing said systems re-map generator to re-map the data of said PRN re-map table.

Claim 9 (previously presented): The pseudo-random key generator according to claim 8, wherein said system re-map generator selectively rearranges data stored in said computer readable storage medium.

Claim 10 (currently amended): A cryptographic communication system having a pseudo-random key generator for generating cryptographic keys, said pseudo-random key generator comprising:

a pseudo-random number generator;

a timing circuit operatively coupled to said pseudo-random number generator, said timing circuit providing a sequence of current timing values;

a first computer readable storage area operatively coupled to said pseudo-random number generator, said first computer readable storage area containing a plurality of data values, each data value associated with a unique storage address within said first computer readable storage area;

a second computer readable storage area operatively coupled to said first computer readable storage area, said second computer readable storage area containing a plurality of key data values, each key data value associated with a unique storage address within said second computer readable storage area,

wherein the pseudo-random number generator periodically generates a pseudo-random number for every predetermined key change period, wherein each generated pseudo-random number is used to look up a unique address in the first computer readable storage area for retrieving the data value associated with the looked up unique address, and wherein the retrieved data value is used to look up a unique address in the second computer readable storage area for retrieving a key value data, said key value data being used to form a cryptographic key,

wherein, upon initialization of the pseudo-random key generator, said timing circuit compares a current timing value with a predetermined crypto midnight initialization timing value and cause the pseudo-random number generator to ~~generate~~ cycle through a set of initialization

pseudo-random numbers starting from the crypto midnight initialization timing value until a pseudo-random number is generated for all of the key change periods between the crypto midnight initialization timing value and the current timing value.

Claim 11 (previously presented): The cryptographic communication system according to claim 10, further comprising a programmed processor operatively coupled to said first computer readable storage area for generating the data values in accordance with a predetermined algorithm.

Claim 12 (previously presented): The cryptographic communication system according to claim 11, wherein said programmed processor selectively rearranges the data values in said first computer readable storage area.

Claim 13 (previously presented): The cryptographic communication system according to claim 10, further comprising a programmed processor operatively coupled to said second computer readable storage area for generating the key data values in accordance with a predetermined algorithm.

Claim 14 (previously presented): The cryptographic communication system according to claim 13, wherein said programmed processor selectively rearranges the key data values in said second readable storage area.

Claim 15 (currently amended): A method of generating cryptographic keys using a pseudo-random number generator, a first computer readable storage area, and a second computer readable storage area, said method comprising the steps of:

inputting into said pseudo-random number generator an initial data value;

initializing said pseudo-random number generator, said step of initialization includes steps of determining a difference between a crypto midnight initialization time value and a current time value, and causing said pseudo-random number generator to ~~generate~~ cycle through a set of initial pseudo-random numerical values;

generating a current time pseudo-random numerical value;

generating a first data string by using said generated current time pseudo-random numerical value to look up a unique memory address in the first computer readable storage area and retrieving a data value associated with the unique memory address in the first compute readable storage area, said data value being one of a plurality of data values stored in the first computer readable storage area; and

generating a second data string by using said first data string to look up a unique memory address in the second computer readable storage area and retrieving a key data value associated with the unique memory address in the second compute readable storage area, said key data value being one of a plurality of key data values stored in the second computer readable storage area,

wherein the retrieved key data value is used to form a cryptographic key.

Claim 16 (previously presented): The method according to claim 15, further comprising the steps of:

rearranging the order of the plurality of data values stored in the first computer readable storage area; and

rearranging the order of the plurality of key data values stored in the second computer readable storage area

Claims 17-22 (canceled)